ICANN 82 COMMUNITY FORUM

# Joint Meeting:
# SSAC-GAC

# Agenda

- Welcome and Introductions
- Quantum Computing and its Impact on Encryption
- Discussion on INFERMAL Study Findings
- Closing Remarks and Next Steps

# Post-Quantum Cryptography (PQC) & DNSSEC: *No one knows the solution yet*

Russ Housley

# ML-DSA is not a good fit for DNSSEC

- Previous Briefing at ICANN 70 by SIDN Labs, University of Twente, TNO, and NLNet Labs
- **Summary**: Module-Lattice-Based Digital Signature Standard (ML-DSA) public keys and signatures simply will not fit in DNS User Datagram Protocol (UDP) messages
- **Maturity**: ML-DSA is a lattice-based signature scheme; not yet as proven as traditional or hash-based signature schemes
- Competition is considering other PQC signature algorithms

➜ So far, none of them have public keys and signatures sizes that are compatible with DNS UDP messages

# Research is Underway

- IRTF PQ DNSSEC Research Side Meetings: Merkle trees are a promising direction, but no standards yet …
- Active research areas and drafts:
  - Stateful Hash-based Signatures for DNSSEC (University of Twente & Verisign)
  - Merkle Tree Ladder (MTL) Mode Signatures (Verisign)
  - SLH-DSA in Merkle Tree Ladder Mode for DNSSEC (Verisign)
- Much more discussion is planned for IETF 122 in Bangkok next week.

# Discussion on INFERMAL Study Findings

Jeff Bedser

# Overview

The report investigates the factors influencing the registration of malicious domains, particularly those used for phishing. It analyzes various features related to domain registration, proactive verification, and reactive security practices.

INFERMAL seems to aim at validating previously anecdotal claims regarding the prevalence of DNS abuse linked to factors such as cost, payment methods, and registration methods. **The report does not offer solutions**; instead, it simply confirms how these factors influence certain rates of DNS abuse. Additionally, it does not discuss the commercial realities associated with domain sales.

**Conclusion: The report highlights the importance of economic incentives, proactive verification, and stringent restrictions in mitigating domain abuse. It provides valuable insights for registrars and policymakers to develop effective anti-abuse strategies.**

# Key Findings

## Economic Incentives

- **Lower Registration Fees**: Each dollar reduction in registration fees corresponds to a 49% increase in malicious domains.
- **Free Services**: The availability of free services, such as web hosting, drives an 88% surge in phishing activities.
- **Discounts**: Discounts on domain registrations are associated with a significant increase in malicious registrations.

## Proactive Measures

- **Stringent Restrictions**: Implementing stringent restrictions can reduce abuse by 63%.
- **API Access**: Registrars providing application programming interface (API) access for domain registration or account creation experience a 401% rise in malicious domains.
- **Verification Practices**: Proactive verification of registrant information, such as email and phone validation, significantly reduces malicious registrations.

# Key Findings

## Reactive Measures

- **Mitigation Times:** The impact of mitigation times on reducing domain abuse is minimal. Even brief uptimes can provide attackers with valuable credentials and financial gain.

## Registrar and TLD Preferences

- **Concentration of Abuse:** Malicious registrations are not uniformly distributed and tend to be concentrated in certain registrars and TLDs.
- **Registrar Practices:** Registrars offering lower prices and free services are more likely to attract malicious registrations.

# Discussion: Pricing and Ease of Access

**Cheaper and easier access** is an incentive for the marketplace of domain acquisition for abusive purposes.

- ➜ This is a basic economic principle—easier acquisition leads to greater demand (even for malicious purposes).
- ➜ What price point deters abuse without hindering legitimate use?

- 2024 Cybercrime Losses (USD): Estimated at $1.03T[1]
- Average Consumer Loss per Phish (USD):
  - Global: $136[2]
  - United States: $3520[1]



1. https://www.gasa.org/post/global-state-of-scams-report-2024-1-trillion-stolen-in-12-months-gasa-feedzai
2. https://aag-it.com/the-latest-phishing-statistics/

# Discussion: Verification Processes

- AI-generated digital identities are now easily accessible and frequently used for identity theft.
  - ➜ What better processes will assist in keeping domains being registered fraudulently?
- Rates of detection from delegation to mitigation valid to measure?
- Would measuring the number of victims per domain be a more helpful metric than number of domains reported?

# Discussion: API Utilization in Registration

- API volume can be driven by Domain Generation Algorithms (DGAs)
- One DGA could account for tens of thousands of domains in one session

➜ Does a metric of 400% increase show that API access is the problem?

# Closing Remarks

Nicolas Caballero, GAC
Ram Mohan, SSAC